

Walsh Sampling with Incomplete Noisy Signals

YI LU

National Research Center of Fundamental Software,
Chinese Academy of Sciences,
Beijing, P.R. China
Dr.yi.lu@ieee.org

Abstract

With the advent of massive data outputs at a regular rate, admittedly, signal processing technology plays an increasingly key role. Nowadays, signals are not merely restricted to physical sources, they have been extended to digital sources as well.

Under the general assumption of discrete statistical signal sources, we propose a practical problem of sampling incomplete noisy signals for which we do not know *a priori* and the sample size is bounded. We approach this sampling problem by Shannon's channel coding theorem. Our main results demonstrate that it is the large Walsh coefficient(s) that characterize(s) discrete statistical signals, regardless of the signal sources. By the connection of Shannon's theorem, we establish the necessary and sufficient condition for our generic sampling problem for the first time. Our generic sampling results find practical and powerful applications in not only cryptanalysis, but software system performance optimization.

Keywords. Walsh transform, Shannon's channel coding theorem, channel capacity, generic sampling, signal processing.

1 Introduction

With the advent of massive data outputs regularly, we are confronted by the challenge of big data processing and analysis. Admittedly, signal processing has become an increasingly key technology. An open question is the sampling problem with the signals, for which we assume that we do not know *a priori*. Due to reasons of practical consideration, sampling is affected by possibly strong noise and/or the limited measurement precision. Assuming that the signal source is not restricted to a particular application domain, we are concerned with a practical and generic problem to sample these noisy signals.

Our motivation arises from the following problem in modern applied statistics. Assume the discrete statistical signals in a general setting as follows. The samples, generated by an arbitrary (possibly noise-corrupted) source F , are 2^n -valued for a fixed n . It is known to be a hypothesis testing problem to test presence of any signals. Traditionally, F is a deterministic function with small or medium input size. It is computationally easy to collect the *complete and precise* distribution f of F . Based on the notion of Kullback-Leibler distance, the conventional approach (aka. the classic distinguisher) solves the sampling problem, given the distribution f *a priori* (see [14]). Nevertheless, in reality, F might be a function that we do not have the complete description, or it might have large input size, or it may be a non-deterministic function. Thus, it is infeasible

to collect the complete and precise distribution f . This gives rise to the new generic statistical sampling problem with discrete incomplete noisy signals, using bounded samples.

In this work, we show that we can solve the generic sampling problem as reliable as possible without knowing signals *a priori*. By novel translations, Shannon's channel coding theorem can solve the generic sampling problem under the general assumption of statistical signal sources. Specifically, the *necessary and sufficient* condition is given *for the first time* to sample the incomplete noisy signals with bounded sample size for signal detection. It is interesting to observe that the classical signal processing tool of Walsh transform [2, 7] is essential: regardless of the signal sources, it is the large Walsh coefficient(s) that characterize(s) discrete statistical signals. Put other way, when sampling incomplete noisy signals of the same source multiple times, one can expect to see *repeatedly* those large Walsh coefficient(s) of same magnitude(s) at the fixed frequency position(s). Note that this is known in application domains such as images, voices. Our results show strong connection between Shannon's theorem and Walsh transform, both of which are the key innovative technologies in digital signal processing. Our generic sampling results find practical and useful applications in not only cryptanalysis – it is expected to become a powerful universal analytical tool for the core building blocks of symmetric cryptography (cf. [11, 15]) – but performance analysis and heterogeneous acceleration. The latter seems to be one of the main bottlenecks for large-scale IT systems in the era of the revolutionary development of memory technologies.

2 Walsh Transforms in Statistics

Given a real-valued function $f : GF(2)^n \rightarrow \mathbb{R}$, which is defined on an n -tuple binary vector of input, the Walsh transform of f , denoted by \hat{f} , is another real-valued function defined as

$$\hat{f}(i) = \sum_{j \in GF(2)^n} (-1)^{\langle i, j \rangle} f(j), \quad (1)$$

for all $i \in GF(2)^n$, where $\langle i, j \rangle$ denotes the inner product between two n -tuple binary vectors i, j . For later convenience, we give an alternative definition below. Given an input array $x = (x_0, x_1, \dots, x_{2^n-1})$ of 2^n reals in the time domain, the Walsh transform $y = \hat{x} = (y_0, y_1, \dots, y_{2^n-1})$ of x is defined by

$$y_i = \sum_{j \in GF(2)^n} (-1)^{\langle i, j \rangle} x_j,$$

for any n -tuple binary vector i . We call x_i (resp. y_i) the time-domain component (resp. transform-domain coefficient) of the signal with size 2^n . For basic properties and references on Walsh transforms, we refer to [7, 11].

Let f be a probability distribution of an n -bit random variable $\mathcal{X} = (X_n, X_{n-1}, \dots, X_1)$, where each $X_i \in \{0, 1\}$. Then, $\hat{f}(m)$ is the *bias* of the Boolean variable $\langle m, \mathcal{X} \rangle$ for any fixed n -bit vector m , which is often called the output *pattern* or *mask*. Here, recall that a Boolean random variable \mathcal{A} has *bias* ϵ , which is defined by $\epsilon = E[(-1)^{\mathcal{A}}] = \Pr(\mathcal{A} = 0) - \Pr(\mathcal{A} = 1)$. Hence, if \mathcal{A} is uniformly distributed, \mathcal{A} has bias 0. Obviously, the pattern m should be nonzero.

Walsh transforms were used in statistics to find dependencies within a multi-variable data set. In the multi-variable tests, each X_i indicates the presence or absence (represented by '1' or '0') of a particular feature in a pattern recognition experiment. Fast Walsh Transform (FWT) is used

to obtain all coefficients $\hat{f}(m)$ in one shot. By checking the Walsh coefficients one by one and identifying the *large*¹ ones, we are able to tell the dependencies among X_i 's.

3 Review on Shannon's Channel Coding Theorem

We briefly review Shannon's famous channel coding theorem (cf. [5]). First, we recall basic definitions of Shannon entropy. The entropy $H(X)$ of a discrete random variable X with alphabet \mathcal{X} and probability mass function $p(x)$ is defined by

$$H(X) = - \sum_{x \in \mathcal{X}} p(x) \log_2 p(x).$$

The joint entropy $H(X_1, \dots, X_n)$ of a collection of discrete random variables (X_1, \dots, X_n) with a joint distribution $p(x_1, x_2, \dots, x_n)$ is defined by

$$H(X_1, \dots, X_n) = - \sum_{\substack{x_1 \\ \dots \\ x_n}} p(x_1, \dots, x_n) \log_2 p(x_1, \dots, x_n).$$

Define the conditional entropy $H(Y|X)$ of a random variable Y given X by

$$H(Y|X) = \sum_x p(x) H(Y|X = x).$$

The mutual information $I(X; Y)$ between two random variables X, Y is equal to $H(Y) - H(Y|X)$, which always equals $H(X) - H(X|Y)$. A communication channel is a system in which the output Y depends probabilistically on its input X . It is characterized by a probability transition matrix that determines the conditional distribution of the output given the input.

Theorem 1 (Shannon's Channel Coding Theorem). *Given a channel, denote the input, output by X, Y respectively. We can send information at the maximum rate C bits per transmission with an arbitrarily low probability of error, where C is the channel capacity defined by*

$$C = \max_{p(x)} I(X; Y), \quad (2)$$

and the maximum is taken over all possible input distributions $p(x)$.

For the binary symmetric channel (BSC) with crossover probability p , that is, the input symbols are complemented with probability p , C can be expressed by (cf. [5]):

$$C = 1 - H(p) \text{ bits/transmission.} \quad (3)$$

We refer to the BSC with crossover probability $p = (1 + d)/2$ and d is small (i.e., $|d| \ll 1$) as an *extremal BSC*. Using

$$H\left(\frac{1+d}{2}\right) = 1 - d^2/(2 \log 2) + O(d^4), \quad (4)$$

we have the following result of the channel capacity for an extremal BSC:

¹Throughout the paper, we refer to the large transform-domain coefficient d as the one with a large absolute value.

Corollary 1 (extremal BSC). *Given a BSC channel with crossover probability $p = (1 + d)/2$, if d is small (i.e., $|d| \ll 1$), then, $C \approx c_0 \cdot d^2$, where the constant $c_0 = 1/(2 \log 2)$.*

Therefore, we can send one bit with an arbitrarily low probability of error with the minimum number of transmissions $1/C = (2 \log 2)/d^2$, i.e., $O(1/d^2)$. Interestingly, in communication theory, this extremal BSC is rare as we typically deal with $|d| \gg 0$ (see [13]).

4 Sampling with Incomplete Noisy Signals

In this section, we put forward two sampling problems (the classical and generic versions). Without loss of generality, we assume the discrete statistical signals are not restricted to a particular application domain. Assume that (possibly noise-corrupted) signals are 2^n -valued. Rather than using the direct signal detection method (as done in specific application domains), we propose to perform the test between the associated distribution and the uniform distribution.

We give the mathematical model on the signal F as follows. F is an arbitrary (and not necessarily deterministic) function. Let X be the n -bit output sample of F , assuming that the input is random and uniformly distributed. Denote the output distribution of X by f . Note that our assumption on a general setting of discrete statistical signals is described by the assumption that F is an arbitrary yet fixed function.

The classical sampling problem can be formally stated as follows. Note that it can be interpreted as the classical distinguisher, though the problem statement of the classical distinguisher is slightly different and it uses a slightly different N (cf. [14]).

Theorem 2 (Classical Sampling Problem). *Assume that the largest Walsh coefficient of f is $d = \hat{f}(m_0)$ for a nonzero n -bit vector m_0 . We can detect F with an arbitrarily low probability of error, using minimum number $N = (8 \log 2)/d^2$ of samples of F , i.e., $O(1/d^2)$.*

The classical sampling problem assumes that F together with its characteristics (i.e., the largest Walsh coefficient d) are known *a priori*. Next, we present our main sampling results for practical (and widely applicable) sampling. Assuming that it is infeasible to know signal F *a priori*, we want to detect signals with an arbitrarily low probability of error and with bounded sample size. Note that the sampled signal is often incomplete (and possibly noisy) and the associated distribution is noisy (i.e., not precise). We call this problem as generic sampling with incomplete noisy signals. In analogy to the classical distinguisher, this result can be interpreted as a generalized distinguisher² in the context of statistical cryptanalysis. We give our main result with $n = 1$ below.

Theorem 3 (Generic Sampling Problem with $n = 1$). *Assume that the sample size of F is upper-bounded by N . Regardless of the input size of F , in order to detect F with an arbitrarily low probability of error, it is necessary and sufficient to have the following condition satisfied, i.e., f has a nontrivial Walsh coefficient d with $|d| \geq c/\sqrt{N}$, where the constant $c = \sqrt{8 \log 2}$.*

Assume that f satisfy the following conditions: 1) the cardinality of the support of f is a power of two (i.e., 2^n), and 2) 2^n is small, and 3) $f(i) \in (0, 3/2^n)$, for all i . Now, we present a generalized result for $n \geq 1$, which incorporates Theorem 3 as a special case:

²With $n = 1$, this appears as an informal result in cryptanalysis, which is used as a black-box analysis tool in several crypto-systems.

Proposition 1 (Generic Sampling Problem with $n \geq 1$). *Assume that the sample size of F is upper-bounded by N . Regardless of the input size of F , in order to detect F with an arbitrarily low probability of error, it is necessary and sufficient to have the following condition satisfied, i.e.,*

$$\sum_{i \neq 0} (\hat{f}(i))^2 \geq (8 \log 2)/N. \quad (5)$$

We note that the sufficient condition can be also proved based on results of classic distinguisher (i.e., Squared Euclidean Imbalance), which uses the notion of Kullback-Leibler distance and states that $\sum_{i \neq 0} (\hat{f}(i))^2 \geq (4 \log 2)/N$ is required for high probability [14]. Secondly, by duality of time-domain and transform-domain signals, the discrete statistical signals can be characterized by large Walsh coefficients of the associated distribution. Thus the most significant transform-domain signals are the largest coefficients in our generalized model.

4.1 Proof of Theorem 3

We first prove the following hypothesis testing result by Shannon's Channel Coding Theorem:

Theorem 4. *Assume that the boolean random variable \mathcal{A} has bias d and d is small. We are given a sequence of random samples, which are i.i.d. following the distribution of either \mathcal{A} or a uniform distribution. We can tell the sample source with an arbitrarily low probability of error, using the minimum number N of samples $(8 \log 2)/d^2$, i.e., $O(1/d^2)$.*

Proof. We propose a novel non-symmetric binary channel. Assume the channel with the following transition matrix

$$p(y|x) = \begin{pmatrix} 1 - p_e & p_e \\ 1/2 & 1/2 \end{pmatrix},$$

where $p_e = (1 - d)/2$ and d is small. The matrix entry in the x th row and the y th column denotes the conditional probability that y is received when x is sent. So, the input bit 0 is transmitted by this channel with error probability p_e (i.e., the received sequence has bias d if input symbols are 0) and the input bit 1 is transmitted with error probability $1/2$ (i.e., the received sequence has bias 0 if input symbols are 1). By Shannon's channel coding theorem, with a minimum number of $N = 1/C$ transmissions, we can reliably (i.e., with an arbitrarily low probability of error) detect the signal source (i.e., determine whether the input is '0' or '1').

To compute the channel capacity C , i.e., find the maximum defined in (2), no closed-form solution exists in general. Nonlinear optimization algorithms (see [1, 3]) are known to find a numerical solution. Below, we propose a simple method to give a closed-form estimate C for our extremal binary channel. As $I(X; Y) = H(Y) - H(Y|X)$, we first compute $H(Y)$ by

$$H(Y) = H\left(p_0(1 - p_e) + (1 - p_0) \times \frac{1}{2}\right), \quad (6)$$

where p_0 denotes $p(x = 0)$ for short. Next, we compute

$$H(Y|X) = \sum_x p(x) H(Y|X = x) = p_0 \left(H(p_e) - 1 \right) + 1. \quad (7)$$

Combining (6) and (7), we have

$$I(X; Y) = H\left(p_0 \times \frac{1}{2} - p_0 p_e + \frac{1}{2}\right) - p_0 H(p_e) + p_0 - 1.$$

As $p_e = (1 - d)/2$, we have

$$I(X; Y) = H\left(\frac{1 + p_0 d}{2}\right) - p_0 \left(H\left(\frac{1 - d}{2}\right) - 1\right) - 1.$$

For small d , we apply (4) in Appendix

$$I(X; Y) = -\frac{p_0^2 d^2}{2 \log 2} - p_0 \left(H\left(\frac{1 - d}{2}\right) - 1\right) + O(p_0^4 d^4). \quad (8)$$

Note that the last term $O(p_0^4 d^4)$ on the right side of (8) is ignorable. Thus, $I(X; Y)$ is estimated to approach the maximum when

$$p_0 = -\frac{H\left(\frac{1-d}{2}\right) - 1}{d^2/(\log 2)} \approx \frac{d^2/(2 \log 2)}{d^2/(\log 2)} = \frac{1}{2}.$$

Consequently, we estimate the channel capacity (8) by

$$C \approx -\frac{1}{4}d^2/(2 \log 2) + \frac{1}{2} \left(1 - H\left(\frac{1-d}{2}\right)\right) \approx -d^2/(8 \log 2) + d^2/(4 \log 2) = d^2/(8 \log 2).$$

□

We now proceed to prove Theorem 3. The only nontrivial Walsh coefficient d for $n = 1$ is $\hat{f}(1)$, which is the bias of F . First, we will show by contradiction that this is a necessary condition. That is, if we can identify F with an arbitrarily low probability of error, then, we must have $|d| \geq c/\sqrt{N}$. Suppose $|d| < c/\sqrt{N}$ otherwise. Following the proof of Theorem 4, we know that the error probability is bounded away from zero as the consequence of Shannon's Channel Coding Theorem. This is contradictory. Thus, we have shown that the condition on d is a necessary condition. Next, we will show that it is also a sufficient condition. That is, if $|d| \geq c/\sqrt{N}$, then, we can identify F with an arbitrarily low probability of error. This follows directly from Theorem 2 with $n = 1$. We complete our proof.

4.2 Proof of Proposition 1

Assume that the channel have transition matrix $p(y|x)$. Let $p(y|x = 0)$ denote the distribution f , and let $p(y|x = 1)$ be a uniform distribution. Denote the channel capacity by C . For convenience, we let $f(i) = u_i + 1/2^n$ for $i = 0, \dots, 2^n - 1$. Note that we have $\sum_i u_i = 0$ and $-1/2^n < u_i < (2^n - 1)/2^n$ for all i .

By Taylor series, for all i , we have

$$\begin{aligned} \log(u_i + \frac{1}{2^n}) &= \log \frac{1}{2^n} + 2 \left(\frac{u_i}{\frac{2}{2^n} + u_i} + \frac{1}{3} \left(\frac{u_i}{\frac{2}{2^n} + u_i} \right)^3 + \dots \right) \\ &\approx \log \frac{1}{2^n} + \frac{2u_i}{\frac{2}{2^n} + u_i}, \end{aligned} \quad (9)$$

as we know $u_i/(\frac{2}{2^n} + u_i) \in (-1, 1)$. And we deduce that with small 2^n , we can calculate

$$\begin{aligned}
-\log 2 \cdot H(f) &= \sum_i (u_i + \frac{1}{2^n}) \log(u_i + \frac{1}{2^n}) \\
&\approx \log \frac{1}{2^n} + 2 \sum_i u_i - \sum_i \frac{2u_i}{2 + 2^n \cdot u_i} \\
&\approx \log \frac{1}{2^n} - \frac{1}{2^{n-1}} \sum_i (1 - \frac{1}{1 + 2^{n-1}u_i}).
\end{aligned} \tag{10}$$

Assuming that $|2^{n-1}u_i| < 1$ for all i (and small 2^n), we have

$$\sum_i \frac{1}{1 + 2^{n-1}u_i} \approx \sum_i \left(1 - 2^{n-1}u_i + (2^{n-1}u_i)^2\right).$$

We continue (10) by $-\log 2 \cdot H(f) \approx \log \frac{1}{2^n} + 2^{n-1} \sum_i u_i^2$. Meanwhile, by property of Walsh transform (cf. [11, Sect.2]), we know

$$\sum_i (\hat{f}(i))^2 = 2^n \sum_i \left(f(i)\right)^2 = 2^n \sum_i u_i^2 + 1.$$

So, we have shown an important result as follows

$$\begin{aligned}
H(f) &\approx n - \frac{2^n}{2 \log 2} \sum_i \left(f(i) - \frac{1}{2^n}\right)^2 \\
&= n - \frac{\sum_{i \neq 0} (\hat{f}(i))^2}{2 \log 2},
\end{aligned} \tag{11}$$

assuming that 1) the cardinality of the support of f is a power of two (i.e., 2^n), and 2) 2^n is small, and 3) $f(i) \in (0, 3/2^n)$, for all i .

Next, in order to calculate C , by (11) we first compute

$$H(Y|X) = p_0 H(f) + (1 - p_0)n \approx n - \frac{p_0 \sum_{i \neq 0} (\hat{f}(i))^2}{2 \log 2}, \tag{12}$$

where p_0 denote $p(x = 0)$ for short. Denote the distribution of Y by D_Y . We have $D_Y(i) = p_0 f(i) + (1 - p_0)/2^n = p_0 u_i + 1/2^n$ for all i . Again we can apply (11) and get

$$H(Y) \approx n - \frac{\sum_{i \neq 0} (\widehat{D_Y}(i))^2}{2 \log 2} = n - \frac{p_0^2 \sum_{i \neq 0} (\hat{f}(i))^2}{2 \log 2}. \tag{13}$$

So, we have

$$I(X; Y) = H(Y) - H(Y|X) \approx \frac{(p_0 - p_0^2) \sum_{i \neq 0} (\hat{f}(i))^2}{2 \log 2}.$$

When $p_0 = 1/2$, we have the maximum $I(X; Y)$, which equals

$$C \approx \frac{\sum_{i \neq 0} (\hat{f}(i))^2}{8 \log 2} = \frac{2^n \sum_i \left(f(i) - \frac{1}{2^n}\right)^2}{8 \log 2}. \tag{14}$$

Consequently, we have $N \geq 1/C$, i.e., $\sum_{i \neq 0} (\hat{f}(i))^2 \geq (8 \log 2)/N$. And this is a necessary and sufficient condition, following Shannon's theorem.

4.3 Discussions on More Generalized Results

Above we consider the case that $f(i)$ is not so far from the uniform distribution. Based on the weaker assumption that 2^n is small and $f(i) = 1/2^n + u_i > 0$ (i.e., $u_i > -1/2^n$) for all i , we now show a more general result. We have

$$H(f) \approx n + \frac{1}{\log 2} \sum_i \frac{u_i}{1 + 2^{n-1}u_i}$$

by (10). Following similar computations we have

$$H(Y|X) \approx n + \frac{p_0}{\log 2} \sum_i \frac{u_i}{1 + 2^{n-1}u_i}, \quad (15)$$

$$H(Y) \approx n + \frac{1}{\log 2} \sum_i \frac{p_0 u_i}{1 + 2^{n-1}p_0 u_i}. \quad (16)$$

So, we obtain the following general result,

$$C \approx \max_{p_0} \frac{1}{\log 2} \sum_i \left(\frac{p_0 u_i}{1 + 2^{n-1}p_0 u_i} - \frac{p_0 u_i}{1 + 2^{n-1}u_i} \right). \quad (17)$$

Recall that if $|u_i| < 2/2^n$ for all i , (17) can be approximated by (14), which is achieved with $p_0 = 1/2$. Specifically, if $|u_i| < 2/2^n$, the approximation for the addend in (17) can be expressed as follows,

$$\left(\frac{p_0 u_i}{1 + 2^{n-1}p_0 u_i} - \frac{p_0 u_i}{1 + 2^{n-1}u_i} \right) \approx 2^{n-1} u_i^2 (p_0 - p_0^2), \quad (18)$$

where we use $\frac{v}{1+v} = 1 - \frac{1}{1+v} \approx 1 - (1 - v + v^2) = v - v^2$ (for $|v| < 1$).

Note that for $|v| > 1$, we have $\frac{v}{1+v} \approx 1 - 1/v + 1/v^2$. We can show that with $2^{n-1}u_i = k > 1$ for some i , the addend in (17) can achieve the maximum when $p_0 = 1/k$, that is,

$$\max_{p_0} \left(\frac{p_0 u_i}{1 + 2^{n-1}p_0 u_i} - \frac{p_0 u_i}{1 + 2^{n-1}u_i} \right) \approx \frac{1}{2^{n-1}} \left(1 - \frac{1}{k} + \frac{1}{k^2} - \frac{1}{k^3} \right). \quad (19)$$

On the other hand, the right-hand side of (18) equals $(p_0 - p_0^2)k^2/2^{n-1}$, which is much larger than (19).

Meanwhile, with $2^{n-1}u_i = k = 1$ for some i , we have

$$\max_{p_0} \left(\frac{p_0 u_i}{1 + 2^{n-1}p_0 u_i} - \frac{p_0 u_i}{1 + 2^{n-1}u_i} \right) \approx \max_{p_0} \frac{1}{2^{n-1}} \left(\frac{p_0}{2} - p_0^2 \right) = \frac{1}{16} \cdot \frac{1}{2^{n-1}}, \quad (20)$$

when $p_0 = 1/4$.

Further, based on Renyi's information measures (cf. [15]), we make the following conjecture for an even more general form of our channel capacity C .

Conjecture 1. *Let Q, U be a non-uniform distribution and a uniform distribution over the support of cardinality 2^n . Let the matrix of T consist of two rows Q, U and 2^n columns. We have the following relation between Renyi's divergence of degree $1/2$ and the generalized channel capacity of degree $1/2$ (i.e., standard Shannon's channel capacity),*

$$D_{1/2}(Q||U) = 2 \cdot C_{1/2}(T).$$

Table 1: Performance estimates for external WHT running on one PC (2.8GHz CPU, 16GB RAM)

L		32	34	36	38	40
disk space		32 GB	128 GB	512 GB	2 TB	8 TB
runtime using	(hrs.)	1.0	5.8	30.5	150.4	715.4
4GB RAM	(days)	0.04	0.24	1.3	6.3	29.8
runtime using	(hrs.)	0.8	5.0	26.9	136.2	658.5
8GB RAM	(days)	0.03	0.21	1.1	5.7	27.4

Table 2: Performance estimates for external WHT running on one PC (2.8GHz CPU, 16GB RAM) with a remote disk

L		32	34	36	38	40
disk space		32 GB	128 GB	512 GB	2 TB	8 TB
runtime using	(hrs.)	1.8	10.5	55.4	274.8	1312.7
4GB RAM	(days)	0.07	0.4	2.3	11.4	54.7
runtime using	(hrs.)	1.4	8.8	48.7	248.2	1206
8GB RAM	(days)	0.06	0.37	2.0	10.3	50.2

Finally, assume that 2^n -valued F has potentially large input space 2^L . The collected distribution of N output samples in the time-domain fits in the noisy model of Sparse WHT [4, 9, 10], supposing that N is sufficiently larger than 2^n . That is, the additive Gaussian noise is i.i.d. and has zero mean and variance $\sigma^2 = 1/(N2^n)$. This can be justified by the following.

Theorem 5. *Given a sequence of N blocks of n bits each, assume that each block is i.i.d. and uniformly distributed. Let the random variable x_i denote the counter for the block value i (for all i) in the sequence. Then, x_i follows the Binomial distribution $\mathcal{B}(N, 1/2^n)$ for all i .*

When N is sufficiently larger than 2^n , $\mathcal{B}(N, 1/2^n)$ can be approximated by the Gaussian distribution $\mathcal{N}(\mu, \sigma^2)$, where the mean $\mu = N/2^n$ and the variance $\sigma^2 = N \times 1/2^n \times (1 - 1/2^n) \approx N/2^n$.

Corollary 2. *Let the time-domain input array $x = (x_0, \dots, x_{2^n-1})$ be defined above and the Walsh transform denoted by $y = \hat{x} = (y_0, \dots, y_{2^n-1})$. Then, for nonzero i , y_i follows the Gaussian distribution $\mathcal{N}(0, N)$ and $y_0 = N$.*

Therefore, sparse WHT will work with our generic sampling problem. Thus, regardless of the value of 2^L , we obtain evaluation time N queries of F , processing time roughly on the order of n , provided that $\sum_{i \neq 0} (\hat{f}(i))^2 \geq (8 \log 2)/N$ (i.e., $\text{SNR} \geq 8 \log 2$).

5 Applications and Experimental Results

We first demonstrate a cryptographic sampling application. The famous block cipher GOST 28147-89 is a balanced Feistel network of 32 rounds. It has a 64-bit block size and a key length of 256 bits.

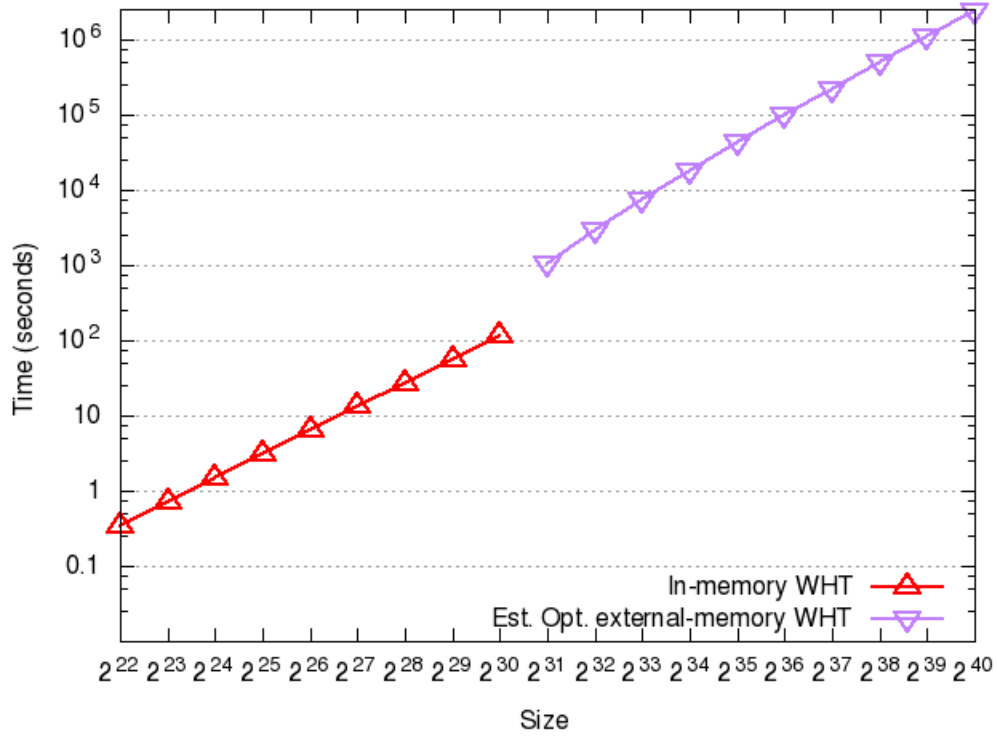


Figure 1: The runtime of scalable WHT computing

Let 32-bit L_i and R_i denote the left and right half at Round $i \geq 1$ and L_0, R_0 denote the plaintext. The subkey for Round i is denoted by k_i . For the purpose of multi-round analysis, our target function is $F(R_{i-1}, k_i) = R_{i-1} \oplus k_i \oplus f(R_{i-1}, k_i)$, where $f(R_{i-1}, k_i)$ is the round function. We choose $N = 2^{40}$. It turns out that, surprisingly, the largest three Walsh coefficients are $2^{-6}, 2^{-6.2}, 2^{-6.3}$ respectively. This new weakness leads to severe various attacks on GOST. Similarly, our cryptographic sampling technique is applicable and it further threatens the security of the SNOW 2.0 cipher [16].

Moreover, our current results show that for general $\text{SNR} \geq 8 \log 2$, regardless of 2^L , when $N \sim 2^n$, we can always choose appropriate b such that $N = b \cdot 2^\ell$ and apply the Sparse WHT technique. Clearly, with $n = 64$, it would become a powerful universal analytical tool for the core building blocks of symmetric cryptography (cf. [11, 15]). In contrast, current computing technology [12] can afford exascale WHT (i.e., on the order of 2^{60}) within 2 years, which uses 2^{15} modern PCs. In Table 1 and Table 2, we list performance estimates for external WHT on a single PC (using the local disk and remote disk respectively). Figure 1 shows optimized WHT performance with respect to 2^n .

Another notable practical application is software performance optimization. Current large-scale IT systems are of hybrid nature. Usually, only partial information about the architecture as well as some of its component units is known. Further, the revolutionary change of the physical components (e.g., memory, storage) inevitably demand that the system take full advantages of the new hardware characteristics. Hence, our sampling techniques would certainly help to solve the problem of performance analysis and optimization for the whole heterogeneous system.

References

- [1] S. Arimoto, An algorithm for computing the capacity of arbitrary discrete memoryless channels. *IEEE Trans. Inform. Theory*, IT-18 14-20, 1972.
- [2] J. M. Blackledge. *Digital Signal Processing – Mathematical and Computational Methods, Software Development and Applications*. Horwood Publishing, England, Second Edition, 2006.
- [3] R. Blahut, Computation of channel capacity and rate distortion functions. *IEEE Trans. Inform. Theory*, IT-18: 460-473, 1972.
- [4] X. Chen, D. Guo, Robust Sublinear Complexity Walsh-Hadamard Transform with Arbitrary Sparse Support, *IEEE Int. Symp. Information Theory*, pp. 2573 - 2577, 2015.
- [5] T. M. Cover, J. A. Thomas. *Elements of Information Theory*. John Wiley & Sons, Second Edition, 2006.
- [6] R. M. Gray, L. D. Davisson. *An Introduction to Statistical Signal Processing*. Cambridge University Press, 2004.
- [7] K. J. Horadam. *Hadamard Matrices and Their Applications*. Princeton University Press, 2007.
- [8] A. Joux. *Algorithmic Cryptanalysis*. Chapman & Hall/CRC, *Cryptography and Network Security*, 2009.
- [9] X. Li, J. K. Bradley, S. Pawar, K. Ramchandran, The spright algorithm for robust sparse Hadamard transforms, *IEEE Int. Symp. Information Theory*, pp. 1857 - 1861, 2014.
- [10] X. Li, J. K. Bradley, S. Pawar, K. Ramchandran, SPRIGHT: A Fast and Robust Framework for Sparse Walsh-Hadamard Transform, *arXiv preprint*, arXiv:1508.06336, 2015.
- [11] Y. Lu, Y. Desmedt, Walsh transforms and cryptographic applications in bias computing, to appear in *Cryptography and Communications*, <http://link.springer.com/article/10.1007/s12095-015-0155-4>, Springer.
- [12] D. A. Reed, J. Dongarra, *Exascale Computing and Big Data - The Next Frontier*, ACM, 2015.
- [13] M. A. Shokrollahi, Personal Communication.
- [14] S. Vaudenay. *A Classical Introduction to Modern Cryptography - Applications for Communications Security*. Springer, New York, 2006.
- [15] S. Vaudenay, A Direct Product Theorem, submitted.
- [16] B. Zhang, C. Xu, W. Meier, Fast correlation attacks over extension fields, large-unit linear approximation and cryptanalysis of SNOW 2.0, *CRYPTO 2015*, LNCS vol. 9215, pp. 643-662, Springer, 2015.